Single Connect Kron

Datasheet

DYNAMIC PASSWORD CONTROLLER

Eliminate Your Risk With Shared Account Password **Management**

There are always **non-personal** accounts within the organizations that have administrative access to the local host and resources, such as administrator for Windows servers, root for Linux/Unix servers, SYSDBA for oracle DBA, admin for Cisco devices, etc. Most of the time, the **passwords** for such local accounts cannot be managed by a central directory server (Active Directory, LDAP) because they are local (designed to be local) on the host. When these passwords are compromised; this represents a **critical threat** for the enterprise.

Shared accounts are not limited to local administrative accounts and there are many shared accounts within an enterprise infrastructure for different user groups, such as for a group of engineers in a specific region, for an enterprise email account (hr@company.com, info@company.com) or social media account of the organization.

Usually, the enterprise's **security policy** requires employees to change the local account password regularly, to use strong passwords, not to share with colleagues but it is often impossible to ensure that it is successful implemented, and any shared accounts are properly protected. With **Dynamic Password Controller** (DPC) you can easily eliminate these security risks of the shared accounts.

Manage Your Passwords in a Central and Secure Vault

Dynamic Password Controller (DPC) removes vulnerability of a privileged shared account by limiting the lifetime of its password, by **verifying** and accounting users and by preserving **passwords** in a secure password vault by not having an agent to be installed on the User PCs or target servers/applications.

The Dynamic Password Controller can manage accounts on following platforms;

Operating Systems: Windows, macOS, Linux and Unix.

Databases: All well-known databases including Oracle, PostgreSQL, MySQL, MSSQL, Cassandra, SAP Sybase, SAP HANA, Teradata

Devices and Appliances with CLI interface that provide password change commands including console access.

Applications: All web-based applications such as SAP, Office 365, Google, AWS, Salesforce, Github, JIRA etc.

Social Media: Facebook, Twitter, LinkedIn, YouTube and other social media applications

Directory Services with LDAP interface.

Single Connect Kron

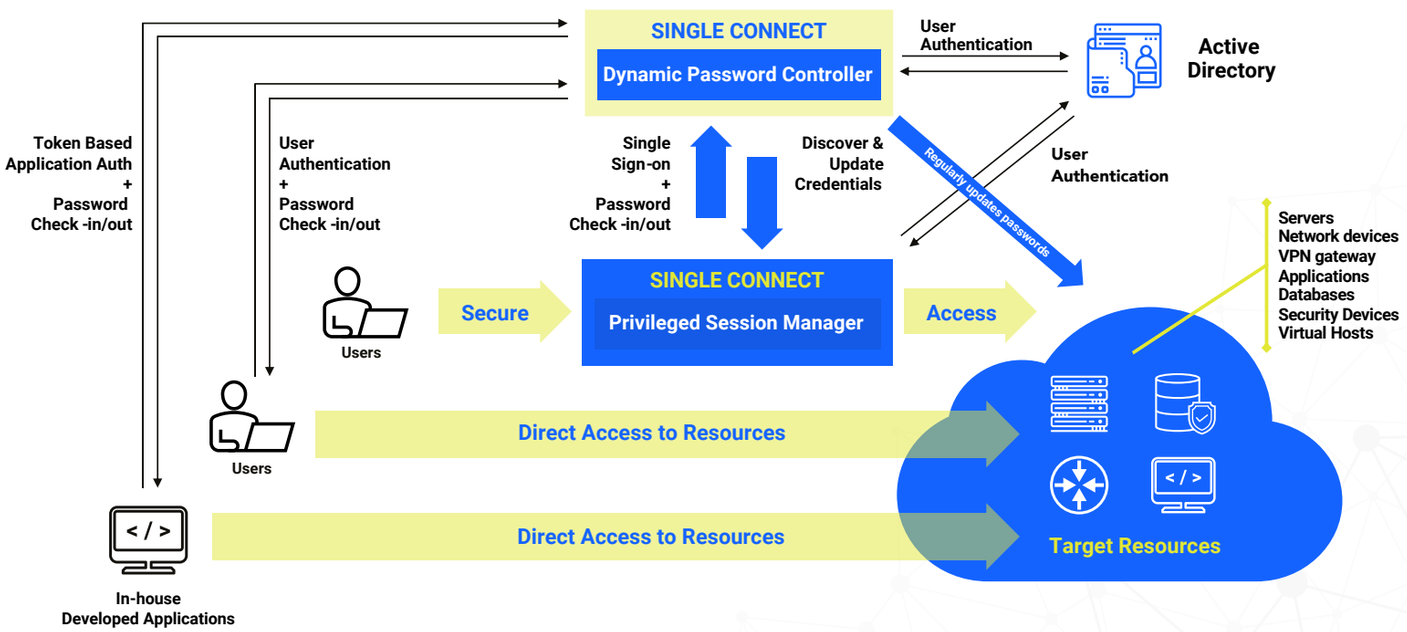
Datasheet

HOW THE DYNAMIC PASSWORD CONTROLLER (DPC) WORKS

As a Centralized Password Vault

Single Connect DPC keeps all **passwords** in a secure, centralized vault, in fully **encrypted** forms and assigns strong and unique passwords to your target hosts, as well as automating **randomization** of your passwords.

DPC's discovery **engine** can discover Windows local and domain accounts, including service accounts, network devices, **virtual platforms** and Linux servers.



Step 1: The User logs in to Single Connect Dynamic Password Controller with his/her ownusername and selects the target host he/she wants to connect to.

Step 2: The Single Connect Dynamic Password Controller releases the target host's password to the User. This password is a One-Time Password (OTP) and is valid for a limited time (e.g. 1 hour). Single Connect ensures logging of entire check-out activity.

Step 3: The User connects directly to the target host and logs in with the password he/she justreceived. Single Connect is not in the middle.

Step 4: At the end of allotted time (e.g. 1 hour), the Single Connect Dynamic Password Controller connects to the target host and changes the password. So, once again, the password is unknown.

Single Connect Kron

Datasheet

AS AN **APPLICATION-TO-APPLICATION PASSWORD** CONTROLLER

Application accounts are used to access databases, connect network devices or other applications, run batch jobs or scripts. The passwords for these accounts are often embedded and stored in unencrypted text files, DB or in source code. Most of the time, these passwords are not changed regularly and can easily be found by people who have access to the server that application runs on, which constitutes a security vulnerability.

Single Connect AADPC enables enterprises to remove these static passwords stored in applications and keep them in DPC,in a secure password vault. Single Connect provides a token-based authentication for the 3rd party applications while accessing password vault. This authentication process verifies the application identity and gives secure access to the password associated with that identity.

Step 1: The Application asks Single Connect AADPC for the password (of a target host) via secure API.

Step 2: After Single Connect successfully authenticates the Application, it delivers the target host's password to the Application via API. This password is a One-Time Password (OTP) and is valid for a limited time (e.g. 1 hour).

Step 3: The Application directly connects to the target host and logs in with the password it just received. Single Connect is not in the middle.

Step 4: At the end of allotted time (e.g. 1 hour), the Single Connect DPC connects to the target host and changes the password. So, once again, the password is unknown.

Single Connect Kron

Datasheet

FEATURES & BENEFITS

Makes sure the real user of the local account is indisputable. **Single Connect** DPC logs which real user checked out the OTP (One-Time Password), along with the beginning and end times.

The passwords are not shared among employees. The password is valid for a limited time and even if an employee shares it, he is still accountable because Single Connect DPC **indisputably** logs which real user checked out the One-Time Password.

The password of the critical systems can be split into pieces by **DPC** so that connection to that systems can be authorized by participation of all users. – **Split** Password

Makes sure strong **passwords** are used for local and service accounts by having Single Connect DPC generate them.

The passwords are stored securely. You never know how and where **employees** store the passwords (sometimes in a text file, sometimes in the cloud), but Single Connect DPC stores the passwords securely, in a vault.

One or **two-level** managerial approval processes can be applied for password check-out. – Managerial Approval

Keep **up-to-date** all services and client applications with new password by having Single connect DPC update them.

Auto lock user account when an employee terminates employment (integration with enterprise **Active** Directory or LDAP is required).

Password **reservation** feature allows users for reserving the password for future usage.

Eliminates usage of **non-expiry** passwords. Single Connect DPC changes the password after **every use** - One-Time Password.

Auto enable new user account with privileges when a new employee starts work (integration with enterprise Active Directory or **LDAP** is required).

Secure vault also stores and manages sensitive information such as **private** passwords, documents and digital identities (SSH keys, certificates and such as digital assets).